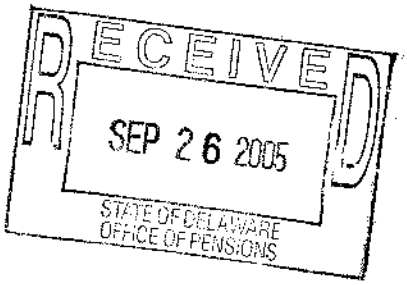
KPMG LLP
1601 Market Street
Philadelphia, PA 19103-2499

Telephone 267 256 7000
Fax 267 256 7200
Internet www.us.kpmg.com



August 30, 2005

Audit Committee of the Board of Pension Trustees
Delaware Public Employees' Retirement System

Gentlemen:

We have audited the financial statements of the Delaware Public Employees' Retirement System (the System), for the year ended June 30, 2005, and have issued our report thereon dated August 29, 2005. In planning and performing our audit of the financial statements of the System, we considered internal control in order to determine our auditing procedures for the purpose of expressing our opinion on the financial statements. An audit does not include examining the effectiveness of internal control and does not provide assurance on internal control. We have not considered internal control since the date of our report.

During our audit we noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarized in Appendix A

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the System's organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

This report is intended solely for the information and use of the Audit Committee of the Board of Pension Trustees, management, and others within the organization and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

Contributions:

Contributions from County/Muni, UD, DSWA

Observation:

We noted during our testwork over employer contributions that information received by certain employers (County/Muni, U of D, DSWA) does not contain payroll information which would allow for a verification of the accuracy/completeness of contributions received from these employers.

Recommendation:

We recommend that the Office of Pensions periodically obtain payroll information which is sufficient to perform a review of the completeness/accuracy of contributions from all employers.

Management Response:

The employers mentioned are manually loaded employers to our retirement system whose payroll and human resource information are received in electronic format on a monthly basis. These reports are reviewed for accuracy of calculation as well as comparison to the funds remitted.

It is our intent to resume on-site audits for these employers for verification of the accuracy of the remitted payroll and human resource transactions.

Reconciliation of contribution information between PeopleSoft, Mercantile and DPERS "All Plans"

Observation:

During our contributions testwork, it was noted that a reconciliation of the employee contribution information contained within PeopleSoft, reported by Mercantile, and accumulated within the DPERS "All Plans" schedule (which is used to create the financial statements) is not performed.

Recommendation:

We recommend that the Office of Pensions periodically perform a reconciliation of contribution information contained with in PeopleSoft, reported by Mercantile and accumulated in "All Plans" to ensure they are all in agreement.

Management Response:

Investment Staff will be performing periodic reconciliations of the contributions as posted in the Mercantile system, DFMS, and CRIS (both the State's interface and through manual data entry by Member Services). Functional support staff has developed queries in CRIS that compile member contribution information by plan for specific periods which can be used by Investments staff to reconcile the plan totals. Monthly reports already exist in DFMS and the Mercantile System for comparison.

Investments

Mercantile Master Trust "Roll-up"

Observation:

During our investments testwork, significant discrepancies between Mercantile "roll-up" information and the DPERS "rollforward", which is based upon monthly Mercantile statements, were noted. Based upon our testwork, individual monthly manger account information was correct, however combined information is not capturing complete and/or accurate data; for example, certain items were posted to the wrong categories. Further, in the absence of reliable reports, manual summation is needed, which allows for human error.

Recommendation:

We recommend that the Office of Pensions continues to work with Mercantile with the ultimate goal of obtaining reliable summary information. Until such time that reliable "roll-up" information can be obtained, a second review should be performed of manual entry information on the "rollforward" to ensure that the data is complete and accurate.

Management Response:

Mercantile has been notified of reporting issues that have been identified during this year's audit process. The Investments staff will be working closely with Mercantile and SunGuard, Mercantile's accounting software vendor, to correct these reporting issues on a forward going basis.

Reconciliation between Mercantile and Investment Managers

Observation:

KPMG noted during investment testwork that a reconciliation of investment information between Mercantile and the investment managers is performed monthly by the investment managers, however a review of reconciliations is only performed when the performance ratios

of the investment manager differ by more than a set percentage from the performance ratios calculated by the Office of Pensions and Ashford Capital Management. Also, formal documentation of the review and resolution of significant reconciling items is not always maintained.

Recommendation:

We recommend that the review of the reconciliations and documentation supporting that review be enhanced. Further, the subsequent month's reconciliation should also be reviewed to ensure that significant reconciling items are resolved in a timely manner.

Management Response:

Investments staff will be working closely with the individual investment managers and Mercantile staff to ensure that all reconciling issues are addressed in a timely manner. All manager reconciliations will be tracked on a monthly reconciliation spreadsheet which will include information regarding any reconciling issues that need to be addressed. It will include documentation of communications between the staff, investment managers, and Mercantile in order to monitor progress and identify areas for future improvement.

Information Technology

Change Control

Observation:

We inquired with personnel responsible for administering changes to the PeopleSoft Pension application and haphazardly selected changes that were made in the production environment, and determined that:

- Minor issues are not always documented, even if the fix requires a system change.
- Documentation does not exist that supports that all changes are authorized, tested, approved, and moved to production by independent personnel.

We also obtained the PeopleSoft security tables and determined that all users assigned to the Information Technology (IT) department role have been granted access to PeopleSoft's development tools in the production environment. We were also informed that access to PeopleSoft production source code directories on the Unix servers is gained through the use of a generic user account to which functional, development, and programming personnel know the password. Without supporting documentation of all changes made to the PeopleSoft environment and limited access to production source code, Management can not be assured of the integrity of the systems and transactions related to the Pension application.

Recommendation:

We recommend that Management implement the STAT Change Control tool as planned. We also recommend that all system changes be documented, tested, and approved prior to implementation. Access to PeopleSoft source code should be limited to production support/operations personnel that do not have access to PeopleSoft development tools to ensure that there is a segregation of duties in place. Additionally, users should be assigned individual Unix accounts to perform daily activities to help ensure some accountability over actions performed.

Management Response:

Implementation of the STAT Change Control tool is 95% complete. The office currently tests and approves all changes prior to production implementation so the STAT product will continue in that vein. Due to the size of the office it is not always possible to separate the access of source code and developer tools but an attempt will be made. The staff will work with DTI to isolate UNIX accounts for individuals.

Information Technology Department Access

Observation:

We obtained the PeopleSoft security tables and examined the security configuration in the production environment and determined that all users assigned to the Information Technology (IT) department role have been granted elevated system administrator-like privileges. Users with this level of access represent a high risk as they can process unauthorized transactions that may circumvent established controls, including the ability to overwrite current and historical transaction records without any audit trial and to administer application security, including adding and changing users and associated roles and permissions.

Recommendation:

We recommend that Management explicitly assign security administration responsibilities and related access permissions so that a segregation of duties exists and user security administration controls cannot be circumvented. We also recommend that IT Department user access to functional or transactional areas in production should be removed. Access to override current or historical records via correction mode should only be assigned to business users with sufficient authority in the organization.

Management Response:

The IT staff will relinquish the super user roles within PeopleSoft security as well as the functional correction capability. The security administrator role will be explored to be placed within a separate area of the IT section.

Default and Generic PeopleSoft User Accounts

Observation:

We obtained PeopleSoft security tables and identified that powerful PeopleSoft delivered and generic super user accounts existed in the production environment. Through our test work we determined that the passwords to these powerful accounts had not been changed from their defaults. These user accounts present a high risk as their passwords can easily be obtained from the internet or guessed, potentially impacting the integrity of the data in the Pension system. We did note, however, that the Pension application is protected by a firewall that restricts access to defined address ranges within the State of Delaware networks.

Recommendation:

We recommend that Management immediately change the passwords for these accounts and evaluate the need for the delivered PeopleSoft accounts. If not needed, the accounts should be locked or removed from the system. If needed, these powerful accounts should have much stronger passwords to help prevent guessing and intrusion.

Management Response:

The delivered PeopleSoft accounts will be investigated for validity and password changes will occur where applicable. If not needed, the accounts shall be locked.

Network System Administration

Observation:

We obtained the network user listings and determined that the account of a former employee' account is still active and being used to perform system administration tasks. We were informed that the password for this account has been changed and is known only to system administrators.

Recommendation:

Because system administrators have full control throughout the system, system administrator privileges should be assigned to individual user accounts to perform daily activities to help ensure some accountability for actions taken. An administrative account should be used only for performing system administration tasks. In addition, we recommend that Management implement policies and procedures to periodically review the ownership of administrative accounts to ensure that no unauthorized administrator assignment is made.

Management Response:

This account represents a past employee who was not on the current network schema. It is felt that rather than have an id listed as Administrator, this would camouflage the identity. We will also investigate assigning the administrator functionality to the network administrator's ids so that accountability is available.

Database Administration

Observation:

We inspected the Pension application database user list and inquired with the database administrators and determined that daily database maintenance activities are performed with a shared system administrator account. Using a shared account to perform daily activities eliminates any accountability for actions performed in the database.

Recommendation:

Database administrators should be assigned individual user accounts that are granted administrative privileges to perform daily activities to help ensure some accountability for database activity. An administrative account should be used only for performing database administration tasks. In addition, we recommend that Management implement policies and procedures to periodically review the ownership of administrative accounts to ensure that no unauthorized administrator assignment is made.

Management Response:

We will share and enforce this recommendation with DTI.

Password Controls

Observation:

We obtained the password complexity settings for the database and Unix operating system and determined that system settings had not been enabled to require complex or strong passwords, including minimum length, expiration, and reusability. We also obtained the password complexity settings for the Windows operating system and noted that the polices do not comply with the *State of Delaware NT Security Policy* (dated September 30, 2003) in regard to minimum password length, invalid login attempts, expiration days, or lockout duration. Windows password complexity settings fall under the responsibility of DTI and DTI management has chosen to implement policy settings at the domain level to provide consistency

of key Windows security settings for all computers and users of the State Domain. This was noted as issue #10 in the State of Delaware, Office of Auditor of Accounts, Department Of Technology And Information William Penn and Biggs Data Center General Controls Follow-Up, Fiscal Year 2005 Information Systems Audit. This issue was scheduled to be resolved by June 30, 2005.

Recommendation:

Passwords are the first line of defense in protecting systems from unauthorized access. There are automated tools freely available on the internet that make guessing passwords a matter of running simple scripts. For this reason, we recommend that Management enable password complexity settings in the database and the Unix operating system that will systematically force users to choose strong passwords. We also recommend that Management work with DTI to ensure that Windows domains are in compliance with prevailing State standards.

Management Response:

We will share and enforce this recommendation with DTI.

Pension Data Backups

Observation:

We were informed that DTI manages the Pension database and that all Pension data is backed up daily to tape and rotated off-site for storage. However, DTI was unable to provide evidence of successful completion of backups as backup logs are not retained once they are verified. DTI was also unable to provide evidence that back up tapes are rotated off-site. If a real time disaster were to occur or if data that was needed was not available, it is undetermined whether the data could be recovered in an acceptable time frame.

Recommendation:

We recommend that Management retain evidence that Pension data is backed up and rotated off-site in accordance with the defined back up policies.

Management Response:

We will share and enforce this recommendation with DTI.

KPMG LLP
1601 Market Street
Philadelphia, PA 19103-2499

Independent Auditors' Report on Internal Control Over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance With *Government Auditing Standards*

Members of the Board of Pension Trustees
Delaware Public Employees' Retirement System:

We have audited the financial statements of the Delaware Public Employees' Retirement System (the System) as of and for the year ended June 30, 2005, and have issued our report thereon dated August 29, 2005. We conducted our audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States.

Internal Control Over Financial Reporting

In planning and performing our audit, we considered the System's internal control over financial reporting in order to determine our auditing procedures for the purpose of expressing our opinion on the financial statements and not to provide an opinion on the internal control over financial reporting. Our consideration of the internal control over financial reporting would not necessarily disclose all matters in the internal control that might be material weaknesses. A material weakness is a reportable condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements caused by error or fraud in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. We noted no matters involving the internal control over financial reporting and its operation that we consider to be material weaknesses. However, we noted other matters including the internal control over financial reporting that have been reported to the management of the System in a separate letter dated August 30, 2005.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the System's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance that are required to be reported under *Government Auditing Standards*.

KPMG

This report is solely intended for the information and use of the Board of Pension Trustees, Secretary of Finance, Office of Pension Management, Office of the Controller General, Office of the Attorney General, Office of the Governor, and the Office of Management and Budget and is not intended to be and should not be used by anyone other than these specified parties. However, under 29 Del C., Section 10002(d), this report is public record and its distribution is not limited.

KPMG LLP

August 29, 2005